

## UNITED STATES DISTRICT COURT

for the

Eastern District of Tennessee

United States of America

v.

Lucas Anthony Nichols

Case No.

3:17-MJ-

2171

---

Defendant(s)

## CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of October 23, 2018, in the county of Knox in the  
Eastern District of Tennessee, the defendant(s) violated:

*Code Section*18 U.S.C. §§ 2252A(a)(2) and  
2252A(a)(5)*Offense Description*Receipt and Distribution of Child Pornography  
Possession of Child Pornography

This criminal complaint is based on these facts:

See Affidavit of Homeland Security Investigations Special Agent Michelle Evans, attached hereto and incorporated herein.

☒ Continued on the attached sheet.

Complainant's signature

Michelle Evans, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/27/2017

Judge's signature

City and state: Knoxville, Tennessee

H. Bruce Guyton, U.S. Magistrate Judge

Printed name and title

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF TENNESSEE  
AT KNOXVILLE**

**In the Matter of the Criminal Complaint in  
United States v. Lucas Anthony Nichols**

**Case No: 3:-17-MJ-**2171

**AFFIDAVIT IN SUPPORT OF COMPLAINT**

I, Michelle Evans, a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), being duly sworn, depose and state the following:

1. I make this affidavit in support of a criminal complaint and arrest warrant for LUCAS ANTHONY NICHOLS (hereinafter "NICHOLS.")
2. In support of the complaint and arrest warrant, I hereby incorporate by reference the facts set forth in my prior affidavit in support of an application for the search warrant in Case No. 3:17-MJ-2168, a copy of which is attached hereto as Exhibit 1.
3. On October 23, 2017, I interviewed NICHOLS in association with the execution of the warrant in Case No. 3:17-MJ-2168, referenced above. NICHOLS admitted that he created the Dropbox, Inc., account referenced in all three Cybertips described in my affidavit in Case No. 3:17-MJ-2168. NICHOLS also admitted that the email addresses "offroadjunkie@live.com" and "lucasanichols@gmail.com" were his email accounts. NICHOLS admitted that he receives child pornography from unknown individuals via a link sent to him on KIK messenger an Internet-based chat application that allows users to communicate and exchange image files. NICHOLS stated that the links contained pornographic depictions of minors under the age of 16 years old. NICHOLS also stated that some of the child pornography videos contained children that were approximately six or seven years old. NICHOLS stated that he trades the child

pornography images with other individuals but could not remember who those individuals were or how many images and videos he had traded. NICHOLS also stated that he has uploaded several of the child pornography images and videos to Dropbox, Inc., Google+, as well as the "Mega" application. NICHOLS stated that he has been viewing, downloading, and/ or uploading child pornography for about a year. NICHOLS also stated that Dropbox, Inc., has terminated an online storage account into which he had uploaded child pornography. NICHOLS stated the last time he viewed child pornography was on October 21, 2017.

4. I have learned that on October 26, 2017, KPD-ICAC Investigator Chris Jones interviewed NICHOLS. NICHOLS admitted to Investigator Jones that about a year ago NICHOLS recorded a video of a minor female taking a shower without the minor female's knowledge. NICHOLS also admitted that about one year ago NICHOLS photographed the vagina of a sleeping 6 to 7 year-old minor female by moving the minor female's undergarments to the side while the minor was asleep.

5. Pursuant to the warrant issued in Case No3:17-MJ-2168, an LG G4 cellular telephone belonging to NICHOLS was seized. A preliminary forensic examination of the LG G4 cellular telephone revealed (20) twenty file images depicting minors engaged in sexually explicit conduct. The (20) twenty images depict children ranging in the ages of (2) two years old to (14) fourteen years old engaged in sex acts. One of the 20 files stored on the LG G4 cellular telephone is named "**a874a57d-3419-4694-981b-54f45fdb86e2.0**" This file is a color video is 30 seconds in length and contains audio. The video depicts a minor Caucasian female that is nude from the waist down and is approximately 2-3 years of age. The video depicts the child lying on her back with her vagina exposed while an adult male penetrates the minor's vagina with his penis.

6. Based on the foregoing, there is probable cause to believe that LUCAS ANTHONY NICHOLS has violated 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5), which make it a crime to knowingly receive or distribute child pornography that has travelled in interstate or foreign commerce, and to knowingly possess child pornography that has traveled in interstate or foreign commerce.

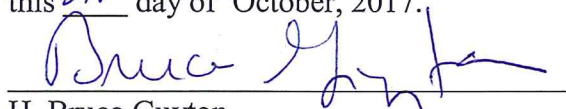
Therefore, I respectfully submit request that the Court issue an arrest warrant for LUCAS ANTHONY NICHOLS.



Michelle Evans  
Special Agent  
Homeland Security Investigations

Sworn and subscribed before me

this 27 day of October, 2017.



H. Bruce Guyton  
UNITED STATES MAGISTRATE JUDGE



UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF TENNESSEE  
AT KNOXVILLE

IN THE MATTER OF THE SEARCH OF  
RESIDENTIAL PROPERTY LOCATED AT  
111 CAVETTON ROAD,  
APARTMENT 25B, KNOXVILLE, TN 37923

3:17-MJ- 2168

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Michelle Evans, a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), being duly sworn, depose and state the following:

1. I have been employed as a Special Agent of HSI since 1995, and am currently assigned to the Office of the Resident Agent in Charge, Knoxville, Tennessee. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have conducted, coordinated, and/or participated in numerous investigations relating to the sexual exploitation of children. I have participated in numerous search warrant executions by HSI, as well as state and local police departments, and have participated in numerous seizures of computer systems and other evidence involving child exploitation and/or child pornography offenses. I have applied for and executed numerous search warrants pertaining to the sexual exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in

enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. This affidavit is made in support of an application for a search warrant for the premises located at 111 Cavetton Road, Apartment 25B, Knoxville, Tennessee 37923, described further in Attachment A (the "SUBJECT PREMISES") for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, which items are more specifically described in Attachment B of this Affidavit.

3. The information contained within the affidavit is based upon information I have gained from my investigation, my personal observations, my training and experience, and/or information related to me by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning the investigation. I have set forth only the facts which I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of 18 U.S.C. §§ 2252 and 2252A are presently located at the SUBJECT PREMISES.

#### **GLOSSARY OF TERMS APPLICABLE TO THIS AFFIDAVIT**

4. COMPUTER STORAGE MEDIA/ DEVICES: A personal computer contains one or more of the following electronic storage media/ devices: 1) A "hard drive" which allows users to read from and write to a hermetically sealed "hard disk". 2) A "floppy drive" that allows users to read from and write to removable "floppy disks". 3) A "compact disk (CD) drive" or "digital video disk (DVD) drive" which allows users to read from and write to super high capacity CD's and DVD's. 4) A "tape drive" which allows users to read from and write to cassette style tapes. 5) "Cellular smartphone telephones" which allows users to place phone calls, has a digital camera, as well as an integrated computer, such as an operating system, internet browsing capabilities,

the ability to run software applications, as well as the ability to store data on the phone. 6)

Various other storage media such as "zip drives", "jazz drives", and "external hard drives" etc. manufactured for the purpose of storing quantities of data in a removable / transportable format. The personal computer uses the permanently installed hard disk, removable floppy disks, CD's, DVD's; zip drives/ jazz drives/ external hard drives to store and retrieve digital information. The disks can contain information critical to the successful start-up and operation of the computer, as well as information defined by and purposely placed by the computer user. Additionally, the disks can contain information that the personal computer places on it transparent to and unbeknownst to the end user that signifies or reveals events that have occurred while the user was using the personal computer. Due to the nature of digital data, information that a computer user deletes from his/ her computer system can remain on the disk indefinitely, and can be recovered and analyzed as easily as existing undeleted information on the disk.

5. INTERNET SERVICE PROVIDER ("ISP"): A company that provides its customers with access to the Internet, usually over telephone lines or cable connections. Typically, the customer pays a monthly fee, and the ISP supplies software that enables the customer to connect to the Internet by a modem or similar device attached to or installed in a computer.

6. THE INTERNET: The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across county, state, and national boundaries.

7. INTERNET PROTOCOL ADDRESS ("IP address"): The unique numeric address of a machine or computer attached to and using the Internet. This address is displayed in four blocks of numbers, as in 123.456.789.001, just for example. Each number can only be used by one computer or machine over the Internet at a time.



8. E-MAIL: Electronic mail transmissions, or "e-mail", include messages distributed by electronic means from one computer user to one or more recipients via a network.

9. INTERNET CLOUD STORAGE: A file hosting service, cloud storage service, online file storage provider, or cyber locker is an Internet hosting service specifically designed to host user files. It allows users to upload files that could then be accessed over the Internet from a different computer, tablet, smart phone, or other networked device, by the same user or possibly by other users, after a password or other authentication is provided. Typically, the service allows HTTP access, and sometimes FTP access. Related services are content displaying hosting services (i.e. video, image and music), virtual storage, and remote backup. Personal file storage services are aimed at private individuals, offering some a sort of "network storage" for personal backup, file access, or file distribution. Users can upload their files and share them publicly or keep them password-protected. Some major providers of Internet cloud storage are Dropbox, SkyDrive, iCloud, and Amazon Cloud Drive.

10. NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN ("NCMEC"): The National Center for Missing & Exploited Children® opened in 1984 to serve as the nation's clearinghouse on issues related to missing and sexually exploited children. Today NCMEC is authorized by Congress to perform 19 programs and services to assist law enforcement, families and the professionals who serve them.

11. CYBERTIP: The CyberTipline receives leads and tips regarding suspected crimes of sexual exploitation committed against children. The CyberTipline is operated in partnership with the F.B.I., Immigration and Customs Enforcement, U.S. Postal Inspections Service, U.S. Secret Service, military criminal investigative organizations, U.S. Department of Justice, Internet Crimes Against Children Task Force program, as well as state and local law enforcement agencies. Reports to the CyberTipline are made by the public and Electronic Service Providers.



ESPs are required by law to report apparent child pornography to law enforcement via the CyberTipline (18 U.S.C. § 2258A). The Knoxville Police Department Internet Crimes Against Children Task Force receives CyberTips from NCMEC on a weekly basis.

12. COMPUTER FILES: Computer files are delineated collections of computer information. These files allow users to collect, organize and store information in meaningful ways on the computer's storage disks. The magnetic disks referred to above contain files with information critical to the successful start-up and operation of the computer, as well as files defined, created and manipulated by the computer user. Additionally, the disks can contain information that the personal computer places on it transparent to and unbeknownst to the end user that signifies or reveals events that have occurred while the user was using the personal computer. Due to the nature of the digital data and personal computer storage techniques, information that a computer user deletes from his/ her computer system can remain on the disk indefinitely, and can be recovered and analyzed as easily as existing undeleted information on the disk.

13. COMPUTER GRAPHIC FILES: Computer graphic files were photographs that have been digitized into computer binary format, or were photographs taken with a "digital" film-less camera that instantly creates the image in computer binary format. Once in that format, the graphic file can be viewed, copied, transmitted, and/or printed. Computer graphic files are differentiated by the type of format convention by which they were created. Two common types of computer graphic files encountered are those in JPEG (Joint Photographic Electronics Group) format having the ".jpg" file extension, and the GIF (Graphic Interchange Format) format having the ".gif" file extension. In addition, there are two primary video graphic files which can display motion picture graphics. The formats encountered are in AVI (Audio Visual Interleaved) format

having the "AVI" file extension, and MPEG (Motion Picture Experts Group) format having the "MPG" file extension. There are also other formats, such as MPEG-4 or MP4.

14. DROPBOX: Dropbox is an Internet cloud storage service operated by Dropbox, Inc. that offers cloud storage file synchronization, and client software. Dropbox allows users to create a special folder on each of their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. Files placed in this folder also are accessible through a website and mobile phone applications.

#### **CONDUCT OF INDIVIDUALS INVOLVED IN CHILD PORNOGRAPHY**

16. Child pornography is not readily available in retail establishments; accordingly, individuals who wish to obtain child pornography do so by ordering it from abroad or by discreet contact with other individuals who have it available.

17. The use of computers to traffic in, trade, collect child pornography and obscenity has become one of the preferred methods of obtaining child pornographic materials. An individual familiar with a computer can use it, usually in the privacy of his/ her home or office, to interact with another individual or a business offering such materials in this country or elsewhere in the world. The use of a computer provides individuals interested in child pornography with a sense of privacy and secrecy not attainable by other media. It also permits the individuals to contact and interact with many more individuals than through the use of the mails.

18. Persons involved in sending or receiving child pornography tend to retain it for long periods of time. The images obtained, traded and/ or sold are prized by those individuals interested in child pornography. In addition to their "emotional" value, the images are intrinsically valuable as trading/ selling material and therefore are rarely destroyed or deleted by the individual collector. Graphic image files can be maintained on the computers built-in hard

drive or storage disks. This tendency is enhanced by the increased sense of security that a computer affords.

### **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

19. I have received specialized training in child sexual/physical abuse as well as child exploitation and child pornography training in reference to criminal investigations. I know all of the below-described information as the result of my training and experience in the investigation of computer-related crime and by conferring with other law enforcement personnel who investigate computer-related crime.

20. I know that computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. They also have revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

21. The advancement in technology of computers, smartphones and tablets has added to the methods used by child pornography collectors to interact with and sexually exploit children. Each of the above serve four functions in connection with child pornography: production, communication, distribution, and storage.



22. Child pornographers can now produce both still and moving images directly from a common video camera, small action style cameras such as a GoPro, smartphones, laptop computers equipped with web cameras, and tablets. In the past, a camera could be attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred, or printed directly from the computer, external hard drive, media card (SD, Compact Flash, micro SD, memory stick), smart phone, tablet, iPod or iPad. As a result of this technology, it is inexpensive and technically easy to produce, store, and distribute child pornography. As an added benefit to the pornographer, this method of production does not leave as large a trail for law enforcement to follow as had been the case in the past. I have been involved in recent investigations where digital cameras, smart phones, tablets and webcams were used to produce child pornography and store said child pornography either on the device, personal computer or removable media of the subject.

23. New technology now allows child pornographers to use even smaller digital devices like smart phones and tablets that have digital cameras and video recording capability built directly into the devices. These devices are equipped with their own processors and memory that allow the devices to actually perform as small mini computers. With the use of free and publicly available apps, a child pornographer has the ability to produce child pornography, receive and distribute it in a matter of just a few seconds and maintain relative anonymity using free open wireless access points.

24. A modem allows any computer to connect to another computer through the use of telephone and/or cable lines. By connecting to a host computer, electronic contact can be made with literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host computers are sometimes operated by commercial



concerns, such as Bellsouth, AT&T and AOL, which allow subscribers to dial a local number and connect to a network which is in turn connected to their host systems. Today many ISPs, such as Comcast Communications and Charter Communications, offer high-speed broadband Internet service. Broadband is often called high-speed Internet because it usually has a high rate of data transmission much higher than the dial-up or DSL structure of the past. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web. Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms" and/or instant messaging.

25. These communication structures are ideal for individuals to possess, receive and distribute child pornography. They provide open and anonymous communication, allowing users to locate other persons who share their interest in child pornography, while maintaining their anonymity. Once contact has been established, it is then possible to send text messages, graphic images, and high-resolution video to other individuals interested in child pornography. Moreover, the child pornographer need not use the large service providers. Child pornographers can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornographers.

26. Because of the proliferation of commercial services that provide electronic mail service, chat services, P2P services and easy access to the Internet, the computer is a preferred method of receipt and distribution of child pornographic materials.

27. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly consisting of hard

drives) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of one terabyte are not uncommon. The Knoxville Police Department's Internet Crimes Against Children Task Force ("KPD-ICAC") computer examiners routinely examine computer hard drives of five hundred (500) gigabytes and more in child pornography cases. These drives can store tens of thousands of images and video at very high resolution and quality. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, save the image, and store it at another location. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful examination of electronic storage devices is it possible to recreate the evidence trail.

28. Based on my knowledge, training and experience and training and experience of other officers, I know that child pornographers commonly download and save some of their collection of child pornography from their computer to removable media such as thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, computer game consoles (Sony PlayStation, Xbox), tablets, iPods or iPads so the images can be maintained in a manner that is both mobile and easily accessible to the collector. It is not uncommon for the child pornographer to print pictures of child pornography and to keep them in a safe and secure location for easy viewing. Thumb drives, CD-ROMs, external hard drives, media cards (SD, Compact Flash, micro SD, memory stick), smart phones, computer game consoles (Sony PlayStation, Xbox), tablets, iPod's or iPads, containing child pornography and printed pictures of child pornography are not only kept near the computer, but also in hidden areas known to the child pornographer, to keep other individuals from discovering the illegal material. For example, a search warrant executed by other officers known to me resulted in the finding of a hard drive wrapped in plastic hidden under a bathroom sink. Additionally, I know



that in 2014, investigators with the KPD-ICAC arrested a subject for the interstate travel to meet a minor for sexual purposes (18 U.S.C. § 2423(a)). An external hard drive was located in the trunk of the suspect's vehicle. After searching the external hard drive pursuant to a search warrant, investigators discovered evidence of sexual abuse with contact on a four-year-old girl, as well as numerous pornographic videos of this sexual abuse produced by the subject utilizing his smartphone.

29. I know that computer technology can be mobile in the form of laptop computers, removable thumb drives, removable hard drives, media cards, computer game consoles, smart phones, iPad's, iPod's, tablets, or accessible via remote or wireless means. Therefore, evidence, contraband, instrumentalities, or fruits of crime can be located virtually anywhere within the residence or vehicle of a child pornographer. I have been involved in child pornography investigations where child pornography was found on removable media located in a suspect's vehicle. Additionally, child pornography can remain on devices indefinitely unless the user takes active steps to delete or overwrite the digital files of child pornography. Additionally, recent investigations have revealed that some suspects, in order to remain safer, have instituted the methodology of downloading child pornography then deleting it after a short period of time. Based on my interviews with child pornographers that utilized the above described method, the suspects indicated they felt an increased level of security knowing the child pornography was not stored on the computer/devices for long periods of time and that they could re-download mass amounts of child pornography at any time. Based on my interviews with child pornographers this methodology gives the child pornographer a greater sense of security. However, computer exams by the KPD-ICAC have revealed that even if the above methodology is utilized, examiners are able to locate and recover evidence about the criminal activity including but not limited to the files' child pornography origin, software used to locate and download child

pornography, and log files identifying specific child pornography files that have been downloaded to the computer system of the suspect.

### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

30. Based on my training and experience, I know that the search of computers and retrieval of data from computer systems and related media, often requires agents to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

(a) Computer storage devices like thumb drives, CD-ROMs, external hard drives, media cards, smart phones, computer gaming consoles, tablets, iPods or iPads can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

(b) Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction, both from external sources



and from a destructive code imbedded in the system such as a "booby trap," a controlled environment is essential to its complete and accurate analysis.

31. Based upon my training and experience and consultation with experts in computer searches, data retrieval from computers, and related media, as well as consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, I know that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all computer system input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

(a) The peripheral devices, which allow users to enter or retrieve data from the storage devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, and/or data security devices are not necessary to retrieve and preserve the data after inspection, the government will return the material within a reasonable time.

(b) In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any

application software, which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

32. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime of advertising, distribution, receipt, and/or possession of child pornography in violation of the law, and should all be seized as such.

33. Based on my training and experience in computer searches and data retrieval from computers while in a laboratory setting, I am aware that such searches can be complex and time consuming.

#### **FACTS SUPPORTING PROBABLE CAUSE TO SEARCH**

34. On September 14, 2017, KPD-ICAC Investigator Chris Jones received Cybertip report number 23749650 from the National Center for Missing and Exploited Children (NCMEC). A review of the Cybertip revealed that Dropbox, Inc., reported to NCMEC that on August 31, 2017 at 19:14:23 UTC a person utilizing the email address "lucasanichols@gmail.com" with the screen/ user name "Lucas Nichols", electronic service provider (ESP) user ID "410337254", and IP address "66.87.152.203" uploaded 109 video files of material depicting child sex abuse/child pornography.

35. Investigator Jones reviewed the video files which were reported to the National Center for Missing and Exploited Children by Dropbox, Inc. The 109 video files were digital computer files in various formats. Based upon Investigator Jones' training and experience, he concluded that these videos depict children, under the age of 18 years old, engaged in sexual acts, posing in various stages of nudity, and/ or lascivious presentation of the child's genitalia. A description of two of the video files are listed below:

36. "10yo japanese girl fingers deep to orgasm with sound"- This file is a color video



that is 4:25 minutes in length and contains audio. The video depicts a young Asian female that is approximately 10-11 years of age. The child is completely nude. The video depicts the child lying on her back with her vagina exposed while the child masturbates.

37. "4b610f6a-971e-4ea7-bd43-159bcbd741d8"- This file is a color video with audio that is 1 minute in length. The video depicts a young Caucasian female that is approximately 3-4 years of age. The child is completely nude with a piece of clothing wrapped around her waist and left leg. The child can also be seen wearing a black mask with eye holes cut into it. The video depicts the child lying on her back while an adult male penetrates her vaginal area with his penis. The child can be heard crying and appears to be in pain.

38. While conducting this investigation of "Lucas Nichols," Investigator Jones learned that in 2015, KPD-ICAC Investigator John Williams received a similar complaint from NCMEC regarding a Dropbox, Inc., account.

39. On October 9, 2015, Investigator John Williams received Cybertip report number 6777265 from NCMEC. A review of the Cybertip revealed that Dropbox, Inc. reported to NCMEC that on August 7, 2015 a person using the email address "offroadjunkie@live.com", Screen/ User Name "Lucas Nichols", ESP User ID "388218613", and IP address "73.190.132.107" uploaded video files depicting child sex abuse/ child pornography. The Cybertip also stated that on September 25, 2015, as well as on October 4, 2015, a person utilizing the email address "offroadjunkie@live.com", Screen User Name "Lucas Nichols", ESP User ID "388218613", and IP address "50.142.96.53" uploaded video files depicting child sex abuse/ child pornography. The Cybertip stated that 108 video files depicting child sex abuse/ child pornography were uploaded during the above described sessions.

40. Investigator Jones reviewed the video files which were reported to NCMEC by Dropbox, Inc., in August 2015. The 108 video files were digital computer files in various

formats. Based upon his training and experience, Investigator Jones concluded that these video files depict children, under the age of 18 years old, engaged in sexual acts, posing in various stages of nudity, and/or lascivious presentation of the child's genitalia.

41. A domain name system (DNS) check on the above described IP addresses through the American Registry for Internet Numbers revealed the IP addresses were registered to Comcast Cable.

42. In October 2015, Investigator Williams issued a State of Tennessee Administrative Subpoena to Comcast Cable in relation to the IP addresses described above in paragraph 39. On October 26, 2015, Investigator Williams received the following information from Comcast Cable, pursuant to the State of Tennessee Administrative Subpoena:

- (a) Subscriber Name: Lucas Nichols**
- (b) Service Address: 111 Cavetton Rd. Apt B  
Knoxville, TN 37923-4114**
- (c) Telephone#: 865-661-4701**
- (d) Types of Service: High Speed Internet Service**
- (e) Account Number: 8396500041270863**
- (f) Start of Service: Unknown**
- (g) Account Status: Active**
- (h) IP Assignment: Dynamically Assigned**
- (i) Current IP Address: See Attached**
- (j) E-mail User Ids: ayanowyn**

43. While conducting this investigation, Investigator Jones learned that on June 29, 2017, Detective Robert Carrigan with the Nashville Metro Police Department received a Cybertip from the NCMEC. A review of that Cybertip revealed that on June 23, 2017, Dropbox, Inc., reported to NCMEC that a person utilizing the email address "lucasanichols@gmail.com" with Screen/User Name "Lucas Nichols", ESP user ID "410337254", and IP address "66.87.152.203" uploaded 77 video files depicting child sex abuse/child pornography to a Dropbox online storage account.



44. Detective Carrigan reported that a review of the video files reported by Dropbox, Inc. to NCMEC, based on his training and experience, revealed that the video files contained predominately nude pre-teen or younger elementary aged girls engaging in sexual acts such as fellatio and penile/ vaginal penetration. Detective Carrigan reported that the children in the video files all appeared to be under the age of 18 years old, most of them between the approximate ages of 3-14 years old.

45. Detective Carrigan reported that an examination of the IP address logs provided by Dropbox, Inc. for recent logins to the reported account showed IP addresses administered by Sprint, Inc., a cellular telephone service/ Internet service.

46. An open source search of the email address "lucasanichols@gmail.com" yielded a Google+ social media profile for "Lucas Nichols" which states that he is an East Tennessee truck driver employed by "Postal Fleet Services" and included a photo of himself. After reviewing the Google+ social media profile, Investigator Williams confirmed that this was the same suspect (Lucas Anthony Nichols) he was investigating at 111 Cavetton Road Apartment 25B, Knoxville, TN 37923 in 2015.

47. A search of www.facebook.com yielded a social media profile for "Lucas Nichols" (www.facebook.com/lucas.nichols.735) which appears to be the same person as the Google+ profile as well as the suspect (Lucas Anthony Nichols) who resides at 111 Cavetton Road Apartment 25B, Knoxville, TN 37923 that Investigator Williams investigated in 2015.

48. On July 3, 2017 Detective Carrigan obtained and executed a judicial subpoena to Sprint, Inc. requesting subscriber information for IP address "66.87.152.76" pursuant to the Cybertip he was investigating. The judicial subpoena also requested subscriber information for all Sprint, Inc. accounts registered to Lucas A. Nichols (DOB: 03/28/78, TN DL#: 081681392) at 111 Cavetton Rd., Knoxville, TN 37923.

49. On July 10, 2017, Detective Carrigan received a response from Sprint, Inc. providing the requested subscriber information. Sprint, Inc. indicated they do not retain logs for IP addresses so were unable to show which user account was assigned the requested IP addresses on the dates requested. Sprint, Inc., did however provide all subscriber information in relation to Lucas A. Nichols. This information is listed below:

**(a) Subscriber Name: Lucas Nichols**  
**(b) Driver's License#: 081681392**  
**(c) Date of Birth: 03/28/1978**  
**(d) Address: 111 Cavetton Road**  
**Knoxville, TN 37923**

50. On July 3, 2017, Detective Carrigan obtained and executed a search warrant to Dropbox, Inc. (ICAC# SW-17-025), requesting the full contents of Dropbox, Inc. account ID "410337254". A Non-Disclosure Order was also signed and included in the search warrant to Dropbox, Inc.

51. On July 13, 2017, Detective Carrigan received a response from Dropbox, Inc., providing the requested account contents. The package contained a password protected flash drive, Certificate of Business Records, and a cover letter from Dropbox, Inc. Detective Carrigan emailed Dropbox, Inc., and was provided a password for the flash drive by Dropbox, Inc. The flash drive contained subscriber information on the account, including a list of device types/models used to access the Dropbox, Inc., account, all of which are through Sprint, Inc. The devices are listed below:

**a) Samsung SM-N900P (Samsung Galaxy Note 3 cellular telephone)**  
**b) Samsung SM-7217S (Samsung Galaxy Tablet)**  
**c) LG LGLS991 (LG G4 cellular telephone)**

52. On October 6, 2017, Investigator Jones contacted United States Postal Inspector

Wallace Bowden. Investigator Jones inquired about whether "Postal Fleet Services" is a

contractor for the United States Postal Service, and whether it employed a "Lucas Nichols" in Knoxville, TN. Inspector Bowden informed Investigator Jones that "Postal Fleet Services" is a contractor for the United States Postal Service and that it does employ a "Lucas Nichols" in Knoxville, TN. Inspector Bowden then sent Investigator Jones a photograph of the "Lucas Nichols" employed by "Postal Fleet Services" and it appears to be the same person photographed in the social media accounts described above as well as the same (Lucas Anthony Nichols) who resides at 111 Cavetton Road, Apartment 25B, Knoxville, TN 37923, and the same suspect in Investigator Williams' investigation in 2015.

53. On October 6, 2017, Investigator Jones conducted a search for "Lucas Nichols" in "Knox County, TN" while utilizing the State of Tennessee Criminal Justice Portal. The search only yielded one response: Lucas Anthony Nichols (Alias), driver's license number: 081681392, Date of Birth: 03/28/1978, 111 Cavetton Rd. Apt. 25B, Knoxville, TN 37923-4114. The driver's license photograph of Lucas Anthony Nichols (Alias) appears to be the same person as the social media photographs described above as well as the photograph supplied by Inspector Bowden. The search also showed that Lucas Anthony Nichols (Alias) has four vehicles registered in his name. The four vehicles registered to Lucas Anthony Nichols (Alias) are as follows: 1990 Blue Ford Bronco (TN tag R68-39K), 1988 Honda Automobile (Unknown tag number), 2014 Jeep Wrangler (TN tag 4F4-0C6), and 2006 Black Ford F-150 (TN tag M01-20D).

54. On October 6, 2017, and October 9, 2017, Investigator Jones conducted surveillance at the apartment complex located at 111 Cavetton Rd., Knoxville, TN 37923 and witnessed the 2014 Jeep Wrangler (TN tag 4F4-0C6), which matches the description and tag number of a vehicle registered to Lucas Anthony Nichols (Alias), parked in front of 111 Cavetton Rd., Apartment Building 25, Knoxville, TN 37923. While conducting surveillance, Investigator Jones also observed a blue Ford Bronco bearing TN tag "91466AA" parked in front of 111 Cavetton



Rd., Apartment Building 25, Knoxville, TN 37923. A records check of this vehicle revealed that it is registered to "Lucas Nichols" at 111 Cavetton Rd., Apt. 25B, Knoxville, TN 37923.

55. A check with the Knoxville Utilities Board shows that Lucas Nichols is currently a subscriber of their electrical services at 111 Cavetton Rd. Apartment 25B, Knoxville, TN 37923 and that he has had service at the same address since April 2015.

56. A check with the Woodlands West Apartments staff revealed that Lucas Nichols is currently a resident at 111 Cavetton Rd., Apartment 25B, Knoxville, TN 37923 and he currently lists "offroadjunkie@live.com" as a contact email address. This is the same email address associated with the original Cybertip reported by Dropbox, Inc. to NCMEC in 2015, where the IP address associated with the reported Dropbox, Inc. account shows registered to Lucas Nichols at 111 Cavetton Rd., Apartment 25B, Knoxville, TN 37923.

#### CONCLUSION

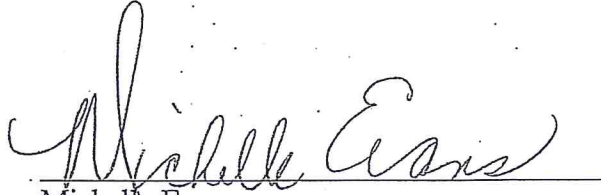
57. Based on the above information, I believe there is probable cause that possession, receipt and distribution of child pornography offenses, in violation of 18 U.S.C. §§ 2252 and 2252A, have been committed, and that evidence, instrumentalities, fruits, and contraband relating to this criminal conduct, as further described in Attachment B, will be found in the SUBJECT PREMISES, further described in Attachment A.

58. Based upon my knowledge, training and experience, and consultations with other Knoxville Police Department Internet Crimes Against Children Task Force investigators, I know that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripheral devices, storage containers, and equipment) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

(a) The volume of evidence: Computer storage devices can store the equivalent of millions of pages of information. For example, one megabyte of magnetic media can store approximately 312 pages of text resulting in a stack of paper 1.6 inches thick. A 40-gigabyte hard drive, could store approximately 12.48 million pages of text resulting in a stack of paper approximately 5,333 feet high. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence of instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be highly impractical to attempt this kind of data search on site.

(b) Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes imbedded as a "booby trap" in the system), a controlled environment is essential to its complete and accurate analysis.

59. Therefore, I respectfully request issuance of the attached search warrant authorizing the search of the premises described in Attachment A and seizure of the items listed in Attachment B.



Michelle Evans  
Special Agent  
Homeland Security Investigations

Sworn and subscribed before me

this 19 day of October, 2017



H. Bruce Guyton  
UNITED STATES MAGISTRATE JUDGE